

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

1           1. (Currently Amended) A method comprising:  
2           modifying an original header associated with an original data packet wherein key  
3           information is added, wherein the modifying an original header further includes identifying at  
4           least one field in the original header for transporting packet assembly information and  
5           replacing the packet assembly information in the field with at least a portion of the key  
6           information;

7           encrypting original data associated with the original data packet in response to the key  
8           information; and

9           forming an encrypted data packet including [[the]] a modified header and [[the]]  
10          encrypted data, wherein the modified header is a same size as the original header.

1           2.       (Previously Presented) The method according to claim 1 further comprising  
2           receiving a unique key identifier associated with the encrypted data packet.

1           3.       (Previously Presented) The method according to claim 2 wherein the  
2           modifying further comprises modifying the original header in response to the unique key  
3           identifier.

1           4.       (Currently Amended) The method according to claim 1 wherein the  
2           modifying further comprises replacing [[the]] a fragmentation identification and a fragment  
3           offset of the original header with a mixing key and an offset.

1           5.       (Original) The method according to claim 1 wherein the original data packet  
2       and the encrypted data packet utilize Internet Protocol version 4.

1           6.       A system comprising:  
2           means for modifying an original header associated with an original data packet  
3       wherein key information is added, wherein the means for modifying an original header further  
4       includes the means for identifying at least one field in the original header for transporting  
5       packet assembly information and replacing the packet assembly information in the field with  
6       at least a portion of the key information;  
7           means for encrypting original data associated with the original data packet in response  
8       to the key information; and  
9           means for forming an encrypted data packet including ~~[[the]]~~ a modified header and  
10       ~~[[the]]~~ encrypted data, wherein the modified header is a same size as the original header.

1           7-9 (Canceled).  
2

1           10. (New) A network encryption method, comprising:  
2           receiving a packet having a packet header and a packet payload;  
3           identifying a first field of the packet header for carrying packet assembly information;  
4           replacing the packet assembly information in the first field with a first encryption  
5       value and a second encryption value;  
6           encrypting original data associated with the packet payload in response to the first  
7       encryption value and the second encryption value; and  
8           forming an encrypted data packet including a modified header and encrypted data,  
9       wherein the modified header has a same size as the packet header.

1           11.     (New) The method according to claim 10, further comprising:  
2           identifying a second field of the packet header for carrying packet assembly  
3           information; and  
4           replacing the packet assembly information in the second field with a third encryption  
5           value.

1           12.     (New) The method according to claim 11, wherein the identifying a first field  
2           of the packet header for carrying packet assembly information includes identifying a fragment  
3           identification in the packet header.

1           13.     (New) The method according to claim 12, wherein the identifying a second  
2           field of the packet header for carrying packet assembly information includes identifying a  
3           fragment offset in the packet header.

1           14.     (New) The method according to claim 13, wherein the replacing packet  
2           assembly information in the first field with a first encryption value and a second encryption  
3           value further includes writing a mixing key refreshing ratio value and a working key refresh  
4           ratio in the first field.

1           15.     (New) The method according to claim 14, wherein the replacing packet  
2           assembly information in the second field with a third encryption value further includes writing  
3           an offset of selecting key value in the second field.

1           16.     (New) The method according to claim 10, further comprising receiving a  
2           unique key identifier associated with the encrypted data packet.

1           17.     (New) The method according to claim 10, wherein the packet and the  
2 encrypted data packet utilize Internet Protocol version 4.

1           18.     (New) The method according to claim 11, further includes activating  
2 checksum in accordance with a checksum field in the packet header after the packet assembly  
3 information in the first and the second fields is replaced with the first, second, and third  
4 encryption values.